REMARKS

The Examiner is thanked for the performance of a thorough search. Submitted concurrently herewith is a Request for Continued Examination (RCE) along with the appropriate fee. By this amendment, Claims 1-3, 6, 16, 18-20, 23, 25-27 and 30 are amended. Claim 17 is canceled. No claims are added or withdrawn. No new matter has been added. Therefore, Claims 1-16 and 18-31 are pending in the application.

Each issued raised in the Office Action is addressed hereinafter.

EXAMINER INTERVIEW

The Examiner is thanked for the interview conducted on September 4, 2008 between Applicants' attorney Adam C. Stone and Examiner Tran. Pending Claim 1 that was rejected in the Office Action was discussed along with U.S. Patent Publication No. 2005/0005017 issued to *Ptacek*. In particular, the discussion focused on the following: the 102 rejection of Claim 1 and the Applicants' proposed amendment to Claim 1. No agreement was reached. No exhibits were shown and no demonstrations were conducted. The Applicant is providing herein the amendment that was proposed during the interview.

CLAIM REJECTIONS – 35 U.S.C. § 102

Claims 1-7 and 16-31 stand rejected under 35 U.S.C. § 102(e) as allegedly anticipated by U.S. Pat. Pub. 2005/0005017 (herein "*Ptacek*"). These rejections are respectfully traversed.

Present Claim 1 features:

> A method of analyzing security events, comprising:
> receiving and processing security events, including grouping the security events into network sessions, each session having an identified source and destination;

> causing display of a graph on a display of a computer system, the graph representing devices in a network, the devices including security devices and non-security devices, the displayed graph including a plurality of individual device symbols and a plurality of group device symbols, each individual device symbol representing a security device of the network and each group device symbol representing a group of non-security devices of the network; and
>
> causing display, in conjunction with the graph, of security incident information including causing display, with respect to a group device symbol, of a security incident volume indicator that indicates a number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to the group device symbol.

(Emphases added). Thus, the method of Claim 1 features, in part, causing display of a graph representing security devices and non-security device in a network. The displayed graph includes a plurality of individual device symbols and a plurality of group device symbols, each individual device symbol representing a security device of the network and each group device symbol representing a group of non-security devices of the network. In conjunction with the graph, the method causes display of security incident information, including causing display, with respect to a group device symbol, of a security incident volume indicator that indicates a number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to the group device symbol.

By doing so, the method of Claim 1 enables, for example, an administrator to easily understand a network's topology and to track down various sources and destinations of network attacks. Such a method is not taught or suggested by *Ptacek*.

In rejecting Claim 1 under 35 U.S.C. § 102(e), the Office Action contends that *Ptacek* anticipates Claim 1. Claim 1 is anticipated by *Ptacek* only if each and every feature as set forth in Claim 1 is found in *Ptacek*. Moreover, the identical invention of Claim 1 must be shown in

Ptacek as in complete detail as is contained in Claim 1. MPEP § 2131. Since each and every feature of Claim 1 is not found in *Ptacek* in as complete detail as is contained in Claim 1 Applicants respectfully request removal of the rejection of Claim 1.

1. <u>Figure 1 of *Ptacek* is not caused to be displayed on the display of a computer screen.</u>

The Office Action equates Figure 1 of *Ptacek* with the claimed "graph." However, the "graph" of Claim 1 is caused to be displayed on a display of a computer system. Figure 1 of *Ptacek* is simply a patent drawing of a computer network. Nothing in *Ptacek* describes a method or system for causing Figure 1 to be displayed on the display of a computer system. *Ptacek* provides no technical description about how to generate a computer display that could contain the things shown in Figure 1. Thus, *Ptacek* does not provide evidence, in as complete detail as is required of a rejection under § 102, "causing display of a graph on a display of a computer system, the graph representing devices in a network." Removal of the rejection of Claim 1 under § 102 is respectfully requested.

2. <u>Even assuming, *arguendo*, that Figure 1 of *Ptacek* was displayed on a display of a computer system, each and every feature of Claim 1 would still not be satisfied by *Ptacek*.</u>

Claim 1 features, *inter alia*,

> causing display, in conjunction with the graph, of security incident information including
>
> > **causing display, with respect to a group device symbol, of a security incident volume indicator that indicates a number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to the group device symbol**.

(Emphasis added). Thus, the method of Claim 1 causes display of a security incident volume indicator with respect to causing display of a group device symbol that represents a group of non-security devices in a network. The displayed security incident volume indicator indicates a number of network sessions whose source or destination is at any member of the group of non-security devices corresponding to the displayed group device symbol. By doing so, the method of Claim 1 enables, for example, an administrator to quickly identify groups of non-security devices that have been involved in a security incident and the volume of security incidents associated with a particular group of non-security devices.

The Office Action appears to equate the drawing labels associated with the firewall devices and the subnets illustrated in Figure 1 of *Ptacek* with the claimed "security incident volume indicator." However, the drawing labels of *Ptacek's* Figure 1 do not in any way indicate "a number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to the group device symbol." The drawing labels of *Ptacek's* Figure 1 are simply reference labels used in the detailed description section of *Ptacek's* patent application to refer to various network elements of the network depicted in Figure 1. The numbers contained in the drawing labels of *Ptacek's* Figure 1 (e.g., "114-1", "SUBNET4", etc.) do not have any relationship to or provide any indication of the number of network sessions associated with the network element that the drawing labels refers to.

Moreover, one skilled in the art could not reasonably equate the drawing labels of *Ptacek* with the "security incident volume indicator" of Claim 1 because one skilled in the art, based on the disclosure of *Ptacek*, could only reasonably interpret the drawing labels of *Ptacek* to be identifiers of drawing elements in a patent application drawing. *Ptacek* provides no genuine technical disclosure about how to generate or use a security incident volume indicator in a computer-implemented method as claimed, and provides insufficient technical evidence for a rejection of the claims. Since *Ptacek* does not disclose, describe, or illustrate the claimed "security incident volume indicator" in as complete detail as contained in Claim 1, the rejection of Claim 1 under § 102 should be withdrawn.

Based on the foregoing, Applicants respectfully submit that each and every feature of Claim 1 is not found in *Ptacek* in as complete detail as contained in Claim 1. Therefore, removal of the rejection of Claim 1 is respectfully requested.

Claims 18 and 25 recite features similar to those recited in Claim 1 except that Claim 18 recites features in the context of a network security events analysis system and Claim 25 recites features in the context of a computer program product for use in conjunction with a computer system. Therefore, Claims 18 and 25 are allowable over *Ptacek* for at least the same reasons provided above that Claim 1 is allowable over *Ptacek*.

3. The Office Action has not alleged that all features of Claim 16 are satisfied by *Ptacek*.

Claims 16 features, *in part*, "receiving and processing a stream of security events, including grouping the security events into a plurality of network sessions, each session having an identified source and destination **and assigned a unique session identifier**." In rejecting Claim 16, the Office Action has not even alleged *Ptacek* satisfies this feature of Claim 16.

Specifically, the Office Action does not identify what thing in *Ptacek* is supposed to be equivalent to the claimed "plurality of network sessions" that are each "assigned a unique session identifier." (*See Office Action*, page 5).

Because the Office Action has not even alleged that all features of Claim 16 are satisfied by *Ptacek* the rejection of Claim 16 under § 102 cannot be maintained. Consequently, removal of the rejection of Claim 16 under § 102 is respectfully requested.

4. Claim 16 recites features similar to those recited in Claim 1 that are also not satisfied by *Ptacek*.

Similar to but not identical to Claim 1, Claim 16 features, in part, "causing display of a graph on a display of a computer system ..." and "causing display, with respect to each group device symbol, of a session volume indicator that indicates a number of identified network sessions whose source or destination is at a non-security device in a group of non-security devices corresponding to the group device symbol."

As explained above with respect to Claim 1, at a fundamental level, *Ptacek* does not describe displaying a graph of security and non-security devices in a network on the display of a computer system and does not describe displaying any type of incident or session volume indicator on a graph of computer network that is displayed on the display of a computer system. Consequently, it is respectfully submitted that Claim 16 recites features that are also not satisfied by *Ptacek*. Removal of the rejection of Claim 16 is respectfully requested.

5. *Ptacek* does not teach or suggest the claimed "second level graph."

Claim 2 depends from Claim 1 and is therefore patentable over *Ptacek* for at least the reasons given above with respect to Claim 1. In addition, Claim 2 recites additional features that independently render it patentable over *Ptacek*.

Claim 2 features, in part:

> upon user selection of a group device symbol for a group of non-security devices, causing display of **a second level graph on the display of the computer system**, **the second level graph** representing the non-security devices in the group and the security devices in association with the group, the displayed **second level graph** including a plurality of non-security device symbols and a plurality of security device symbols, each non-security device symbol representing one non-security device in the group and each security device symbol representing one security device in the group; and

> causing display, in conjunction with the second level graph, of security incident information, including causing display, with respect to a non-security device symbol, of a security incident volume indicator that indicates a number of network sessions whose source or destination is at the non-security device.

(Emphasis added). Thus, Claim 2 relates to displaying a "drill down" graph on the display of a computer system that enables, for example, an administrator to easily discern which non-security devices of a group of non-security devices are involved in a security incident. The method of Claim 2 provides the "drill down" second level graph upon user selection of a group device symbol for a group of non-security devices. The method of Claim 2 is not taught or suggested by *Ptacek*.

The Office Action relies on Figure 2 of *Ptacek* for disclosing the "second level graph" of Claim 2. The Office Action is incorrect. Nothing about *Ptacek* suggests that Figure 2 is displayed on the display of a computer screen. However, even if Figure 2 of *Ptacek* were displayed on the display of a computer screen, it would not satisfy the "second level graph" of Claim 2. In particular, nothing in *Ptacek* describes Figure 2 being displayed "upon user selection of a group device symbol for a group of non-security devices." Figure 2 of *Ptacek* is simply a patent drawing and no reasonable reading of *Ptacek* can contend that Figure 2 is "displayed" upon user selection. This is not a matter of “interpreting” *Ptacek*; the reference simply does not disclose the claimed computer-implemented displaying and no skilled artisan would understand *Ptacek* to describe how to display with a computer the things shown in Figure 2.

Furthermore, there is nothing in Figure 2 of *Ptacek* that one skilled in the art would reasonably equate with the claimed "security incident volume indicator that indicates a number of network sessions whose source or destination is at the non-security device." The Office Action equates the drawing labels "firewall 1", "firewall 2", and "firewall 3" as shown on Figure

2 of *Ptacek* with the claimed "security incident volume indicator." However, similar to the patent drawing labels of Figure 1 of *Ptacek* that the Office Action equated with the "security incident volume indicator" of Claim 1, nothing about the drawing labels of Figure 2 of *Ptacek* indicates "a number of network sessions whose source or destination is at the non-security device."

Based on the foregoing, Applicants respectfully submit Claim 2 recites additional features that independently render it patentable over *Ptacek.*

Claims 19 and 26 recite additional features similar to those additional features recited in Claim 2. Therefore, Applicants respectfully submit that Claims 19 and 26 also recite additional features that independently render them patentable over *Ptacek.*

6. The remaining claims are patentable over *Ptacek.*

The pending claims not discussed so far are dependant claims that depend on an independent claim that is discussed above. Because each dependant claim includes the features of claims upon which they depend, the dependant claims are patentable for at least those reasons the claims upon which the dependant claims depend are patentable. Removal of the rejections with respect to the dependant claims and allowance of the dependant claims is respectfully requested. In addition, the dependent claims introduce additional features that independently render them patentable. Due to the fundamental differences already identified, a separate discussion of those features is not included at this time.

CONCLUSION

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

Please charge any shortages or credit any overages to Deposit Account No. 50-1302.

Respectfully submitted,

Hickman Palermo Truong & Becker LLP

Date: September 18, 2008

/AdamCStone#60531/
Adam Christopher Stone
Reg. No. 60,531

2055 Gateway Place, Suite 550
San Jose, California 95110-1089
Telephone No.: (408) 414-1080 ext. 231
Facsimile No.: (408) 414-1076